Nuvento
Redefining Digital Business

# Keep your Azure environment safe with these 100 Azure security best practices

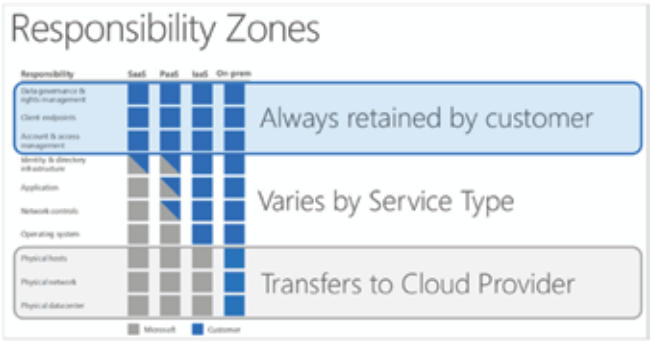
Follow this checklist of 100 security best practices. Your cloud security teams can go through this checklist to cover all security bases and keep your Azure environment safe.

## Azure Security Center best practices

☐ 01. Practice the shared responsibility model

A deep understanding of the division of responsibilities between Azure and your enterprise is critical. Security on public cloud is a shared responsibility. The responsibility for every aspect of your security depends on the cloud model you've chosen – SaaS, PaaS or IaaS. On a high level, you are responsible for your data and managing access to that data.

Depending on the model you choose, your responsibilities will change. Whether you're planning a move to the cloud, or have already moved; a deep understanding of the shared responsibility model is imperative to the success of your Azure Security model.




☐ 02. Keep your identity secure with Azure Active Directory

Identity is fast becoming one of the primary security factors for enterprises.

Microsoft has made several recommendations around securing users' identity with Azure Active Directory.

Azure relies on Azure Active Directory for authentication and these practices are critical to the security of enterprises' Azure Cloud.

To manage identities in a unified manner in a hybrid identity scenario, integrate on-premises and cloud directories with Azure Active Directory Connect. Azure Active Directory also provides Single Sign-On (SSO) when integrated with on-premises Active Directory. With SSO, users need just one set of login credentials as compared to multiple passwords, that could increase the possibilities of weak or reused passwords.

☐ 03. Check suggested changes and alerts on the Azure Security Center

For security on Azure, Azure Security Center is the best way to get started. Azure Security Centers gives users suggestions for changes and alerts for protecting the user's Azure resources. Checking the portal regularly and taking prompt action helps to remediate as many alerts as possible.

Using the Azure Secure Score recommendations, you can visualize your security state and improve your security posture. For your hybrid cloud workloads, you can use Azure Defender. Azure Defender integrates with Azure Security Center and protects your hybrid cloud workloads including servers, data, storage, containers and IoT.

☐ 04. Control the number of subscription owners

Do not have more than three users with owner permissions.

The best practice is to have two trusted Azure administrators who will be the owners of your Azure subscriptions, and one extra account to manage any emergencies.

### ☐ 05. Keep your virtual machines updated

Microsoft recommends system updates for VMs in Azure. Azure's update management solutions automate updates for Windows Virtual Machines.

To ensure that you do not miss critical security updates as well get update support, use Azure Security Center.

### ☐ 06. Keep tabs on network access

Network access is a critical control point on Azure. It's a best practice to have multiple layers of security around and between protected resources.

The first security layer would include a firewall, such as Azure Firewall or a third-party virtual network appliance solution. This layer encompasses security measures like Firewall policies, Distributed Denial of Service (DDoS) prevention, intrusion detection and intrusion prevention systems (IDS/IPS), Web Content Filtering and Vulnerability Management, such as Network Anti-Malware, Application Controls and Antivirus.

The second layer is a Network Security Group (or NSG) to filter network traffic to and from Azure resources in an Azure virtual network. Use the NSG to stop unwanted traffic from entering or leaving an Azure subnet. NSGs for network access help to establish a security zone in an otherwise free-to-communicate structure.

The third layer is an NSG applied to virtual machine network interface. This will allow for control of traffic to and from the virtual machine.

The fourth layer is to opt for ExpressRoute ad site-to-site connections. It is best to avoid an internet connection with a dedicated WAN connection.

### ☐ 07. Remove remote access to virtual machines

Provide users with secure dedicated connections like VPN or ExpressRoute connections (mentioned above) for RDP and SSH access using Just-in-Time (JIT) virtual machine access.

JIT virtual machine access controls inbound traffic to Azure Virtual Machines, reducing Brute Force attack exposure, providing easy access to connect to virtual machines via Remote Desktop or Secure Shell.

### ☐ 08. Keep your sensitive data safe

Protecting your data in the Microsoft Azure cloud – such as keys, secrets and certificates – is critical in safeguarding sensitive data.

Azure Key Vault can be used to keep cryptographic keys and secrets that cloud applications and services use protected.

### ☐ 09. Protect data with encryption

Data at rest and in transit can be protected with encryption. If encryptions are not enabled by default, manually enable them.

Also implement Azure SQL database transparent data along with Azure SQL to protect your database.

## Azure security policy best practices

### ☐ 10. Activate security data collection provision

Enabling automating provisioning of monitoring agent to collect security data lets the Azure Security Center provision the Microsoft monitoring agent on all supported Azure virtual machines and newly created ones.

### ☐ 11. Enable OS vulnerabilities recommendations

Enabling this setting analyzes operating system configurations every day to determine issues that could make the VM vulnerable to an attack.

### ☐ 12. Endpoint protection activation

Activating the endpoint protection recommendations enables Azure Security Center to recommend endpoint protection to be provisioned for all Windows virtual machines to help identify malicious software.

### ☐ 13. Web application firewall (WAF) activation

Keeping the web application firewall switched on lets you monitor attacks against your web applications by using a real-time WAF log.

The application gateway WAF can be integrated with Azure Security Center for a central view of the security state of all Azure resources.

☐ 14. Keep next generation firewall on

Next generation firewalls for virtual machines extend network protections beyond the network security group. Security Center will find where a next generation firewall needs to be set up and enables users to create a virtual space.

☐ 15. Check vulnerability assessments

Enabling vulnerability assessments has Azure Security Center recommending that users install a vulnerability assessment solution on your VM.

☐ 16. Encrypt your storage

When you encrypt your storage, new data in Azure Blobs and Files will be encrypted.

☐ 17. Have SQL auditing and threat detection in place

Once the SQL auditing and threat detection recommendations are enabled, the Azure Security Center recommends that auditing of access to Azure Database be enabled. This is the Azure security best practice for compliance, advanced threat detection and post-incident forensic investigations.

☐ 18. Ensure SQL encryption is enabled

When SQL encryption recommendations setting is enabled, Azure Security Center recommends that encryption at rest be enabled for the Azure SQL Database, its associated backups and transaction logs. This way, even if data is breached, database would not be.

☐ 19. Security contact email and phone number

Providing a security contact email and phone number ensures you are made aware of potential compromise for timely incident response.

☐ 20. Email on alerts to subscription owners

Subscribers must ensure they enable the alerts emails to security contacts and subscription owners. This keeps owners aware of potential compromise for speedy response.

## Securing identity and access management

☐ 21. Multi-factor authentication for all users

Enabling multi-factor authentication for all users who need to access Azure resources provides additional assurance that the individual attempting to gain access is who they claim to be.

With multi-factor authentication, the possibility of an attacker compromising on more than one different authentication methods is much higher, making a compromise more difficult and reducing risks.


☐ 22. Keep guest users to NIL

Add guest users to your account only if it there is a real business need. When you add a guest user, it risks opening access to your resources unnoticed, leading to potential vulnerabilities.

☐ 23. Disable remember multi-factor authentication for devices

Do not give users the option to bypass multi-factor authentication. This option allows users to sign into a device without authentication for a set number of days after a successful sign in using MFA. While this step enhances the users' experience, it also increases the chance of compromise affecting security.

☐ 24. Set number of reset methods to 2

Always have two alternate forms of identification before allowing a password reset. Dual identification is one way to confirm the user's identity.

☐ 25. Enable authentication information re-confirmation

If authentication re-confirmation is disabled, users will not be prompted to reconfirm existing authentication information. While enabled, if a malicious user types in new authentication information, the password reset information will go to the previously registered authentication information, alarming you of the suspicious login attempt.

☐ 26. Enable password reset notifications

Users must be notified of password resets on their primary and secondary emails. This method helps the user to recognize unauthorized password reset activities.

☐ 27. Enable setting to notify all admins if one admin resets the password

Ensure one admin's password reset attempt triggers a notification to all admins. This way, any password reset activity will send out a notification to all administrators so that they can confirm if such a reset is a commonly followed practice within the group.

In certain cases, all administrators change their password every 30 days. Password changes made by a certain admin before the set period may need to be looked into.

☐ 28. User consent to apps that access company data must be disabled

Administrators need to provide consent for all apps a user uses before use. Unless you have an Azure AD as an identity partner with all third-party applications listed, do not allow users to use identity outside your cloud environment.

☐ 29. Ensure adding gallery apps to access panel option is set to 'no'

Admins must provide consent for any app before use. Unless you have an Azure AD as an identity partner for third-party apps, do not allow users to use their identity outside the cloud environment.

☐ 30. User registration on applications must be disabled

The recommended way to use custom-developed applications in an enterprise is to have administrators register it.

This way, the application undergoes a security review before exposing active directory data.

☐ 31. Make sure guest users have limited permissions

If guest access is limited, guests would not have permissions for most directory tasks. This is a good way to reduce risks of unauthorized access.

☐ 32. Disable member invitation options

Allow invitations only through administrators. This ensures only authorized accounts have access to cloud resources.

☐ 33. Disable guest invitation options

Do not allow guests to invite users. Restricting invitations through administrators ensures only authorized accounts have access to cloud resources.

☐ 34. Ensure restricted access to Azure AD admin portal

Allow only administrators to access the Azure AD admin portal. Azure AD holds sensitive data and should have restricted access to avoid exposure to malicious actors.

☐ 35. Disable self-service group management

Allow only administrators to create groups. Self-service group management enables users to create and manage security groups or Office 365 groups in Azure AD.

☐ 36. Disable user security group creation

Allow only administrators to create security groups. Enabling this option allows users to create their own security groups and add members, which increases risks.

☐ 37. Disable security group management

Allow only administrators to manage security groups. This way, users won't be able to make any changes to security groups.

☐ 38. Disable Office 365 group creation

Restrict Office 365 group creation to admins alone. This ensures the creation of such groups does not get out of hand.

☐ 39. Disable Office 365 group management

Restrict Office 365 group management to admins alone. This ensures the management of such groups does not get out of hand.

☐ 40. Enable all user groups for centralized administration

Enable all user groups for centralized administration of all users. This is an easy way to assign the same permissions to all groups in your directory.

You can grant all users in your directory access to a SaaS application by assigning its access to all users' dedicated group. This creates a common policy for all users.

☐ 41. Enable multi-factor authentication to join devices

Adding devices to the Azure AD should go by multi-factor authentication. This ensures unauthorized devices are not added to the directory for a compromised account.

☐ 42. Have a single Azure AD instance for corporate accounts

Establishing a single AD instance brings in consistency and a single authoritative source in a hybrid work environment, increasing clarity and reducing security risks from human errors and configuration complexity.

☐ 43. Integrate on-premises directories with Azure AD

Synchronizing your on-premises directory with the cloud directory using Azure AD Connect.

☐ 44. For new app development, use Azure AD for authentication

Use Azure AD for employees, Azure AD B2B for guest users and external partners and Azure AD B2C to control customer access.

☐ 45. Turn on password hash synch

Password hash synchs user password hashes from an on-premise AD instance to a cloud-based Azure AD instance. This synch helps to protect against leaked credentials being replayed from previous attacks.

☐ 46. Manage connected tenants

Ensure you have visibility into all your subscriptions connected to your production and network environments. Using elevated access, a global administrator in Azure AD can see all subscriptions and manage all groups connected to their environment. Once the risks are assessed, the elevated access must be removed.

☐ 47. Manage and control access to corporate resources

Configure Azure AD conditional access based on a group, location and application sensitivity for SaaS apps and Azure AD-connected apps.

☐ 48. Block legacy authentication protocols

Attackers exploit weaknesses in older protocols every day, for password spray attacks. Configure conditional access to block legacy protocols.

## Storage best practices

☐ 49. Enable secure transfers

Keep data encrypted during transfers. The secure transfer enhances storage security by allowing requests only from secure accounts.

Calling REST APIs to access your storage accounts is possible only when you connect using HTTPS. HTTP requests will be rejected.

☐ 50. Enable storage service encryption

Enable data encryption at rest for blobs. Storage service encryption keeps data at rest protected. Data written in data centers is encrypted in Azure Storage and is automatically decrypted when it is accessed.

## SQL best practices

☐ 51. Enable auditing on SQL servers

Auditing keeps track on SQL servers and writes them to an audit log. This helps in maintaining regulatory compliance, understanding database activity and detecting anomalies.

☐ 52. Set blob as auditing type on SQL servers

Blob-based auditing allows users to perform database object-level auditing.

☐ 53. Enable threat detection on SQL servers

Threat detection on SQL servers gives a new layer of security to detect and respond to potential threats as they occur. Suspicious database activity will raise a trigger.

SQL Threat Detection alerts provide details of suspicious activity and recommends action on how to investigate and mitigate the threat.

☐ 54. Enable all types of threat detection on SQL servers

Enabling all threat detection types protects you against SQL injection, database vulnerabilities and other suspicious activities.

☐ 55. Enable the option to send alerts via email for threats on SQL servers

Saving an email address to which alerts of suspicious activities on SQL servers are sent ensures any threats detected are reported quickly, improving the chances of risk mitigation.

☐ 56. Enable email service and co-administrators to receive SQL server security alerts

Providing an email address to receive alerts ensures that threats detected on SQL servers are reported quickly, improving the chances of risk mitigation.

☐ 57. Enable SQL server firewall rules

Firewalls help to prevent all access to data servers unless the system has specific permissions. Firewalls grant access to databases based on the originating IP address of each request.

☐ 58. Enable auditing on SQL databases

Auditing SQL databases tracks events in the database and writes them in an audit log in Azure.

☐ 59. Enable threat detection on SQL databases

SQL threat detection adds a security layer enabling customers to detect and respond to threats by providing security alerts on anomalous activities.

☐ 60. Enable all types of threat detection on SQL databases

Enabling all threat detection types helps protect against SQL injection, database vulnerabilities and other anomalous activities.

☐ 61. Enable the option to send alerts via email for threats on SQL databases

Saving an email address to which alerts of suspicious activities on SQL databases are sent ensures any threats detected are reported quickly, improving the chances of risk mitigation.

☐ 62. Enable email service and co-administrators to receive SQL database security alerts

Providing email address to receive alerts ensures that threats detected on SQL databases are reported quickly, improving the chances of risk mitigation.

☐ 63. Azure SQL Database transparent data encryption

Protect your SQL database against threats of malicious activities by performing real-time encryption

and decryption of the database, associated backups and transaction log files at rest without any change to the application.

☐ 64. Discover, classify and label the sensitive data in the databases

Classify the data in your SQL database by enabling Data Discovery ad classification in Azure SQL Database. You can monitor access to sensitive data in the Azure dashboard or download reports.

## Virtual machine best practices

☐ 65. Install virtual machine endpoint protection

Installing endpoint protection systems for real-time protection capabilities helps to identify and remove viruses, spyware and other malicious software. With configurable alerts, users know when malicious players attempt to install itself and run-on Azure systems.

☐ 66. Update OS patches for VMs

Windows and Linux VMs should be updated to address bugs/flaws, improve OS/app stability and fix a security vulnerability.

☐ 67. Encrypt data disks on VMs

Keep data disks encrypted where that is a possibility. Encrypting IaaS VM data disks (non-boot volume) keeps its content unrecoverable with a key and keep the volume protected from unauthorized access.

☐ 68. Install VM agent on VMs

Installing VM agents on Azure VMs enables Azure Security Center to collect data. Data is collected from VMs to assess their security state, provide security recommendations and alert to threats.

☐ 68. Rapidly apply security updates to VMs

Enable Azure Security Center to identify missing security updates and apply them.

☐ 70. Deploy and test backup solutions

Production workloads moved to Azure should integrated with existing backup solutions when possible.

☐ 71. Use key encryption key (KEK) for an additional layer of security

Azure Disk Encryption uses the key to wrap encryption secrets before writing to Key Vault

☐ 72. Keep key vault and VMs in the same location

Create and use a key vault that is in the same region as the VM to be encrypted

☐ 73. Take a snapshot/backup before disks are encrypted

Backups provide a recovery option if an unexpected failure happens during encryption.

## Other best practices

☐ 74. Remove deprecated accounts from the subscription

Deprecated accounts are those deployed to your subscription for the trial purposes. Once these accounts are not in use, the best practice would be to have them removed or they could pose a risk if present in any role on the subscription.

☐ 75. Do not grant permissions to external accounts

Non-Azure Directory accounts present on your subscription subject cloud assets to undue risk. So, the best practice is to restrict access to users with external accounts.

☐ 76. Do not use service accounts for subscriptions

Service accounts are not MFA protected and therefore, should not be used for subscription-based activities. Service accounts used in a privileged role expose it to 'credential-theft' related attacks.

☐ 77. Configure Azure Security Center correctly

Security Center in Azure helps with important central settings for your subscription. Configuring Security Center gives a baseline layer of protection for the subscription and commonly used resource types.

☐ 78. Resolve all pending Azure Security Center alerts

Azure Security Center raises alerts based on the policies enabled in the subscription. It is best to resolve these promptly to eliminate exposure to attacks.

☐ 79. Do not make Service Principal Names (SPNs) owners or contributors on the subscription

SPNs have a single credential and in most of their use cases are not MFA protected. So, it's best to avoid adding SPNs to a subscription as owners or contributors.

☐ 80. Protect critical application resources with a resource lock

A resource lock prevents resources from getting deleted accidentally. Proper RBAC (role-based access control) configurations let users set up critical resources in a subscription in such a way that people cannot delete them.

☐ 81. Secure the cloud subscription

It takes a secure subscription to provide a core foundation on which subsequent development and deployment activities can be conducted.
Users should be able to deploy and configure security in the subscription, including elements like alerts, ARM policies, RBAC, Security Center policies, JEA, Resource Locks, etc.

☐ 82. Review all identities in your subscription

Users in the group that do not have legitimate business reason to be present increase your risk surface. By carefully reviewing and removing accounts that shouldn't be there, attacks stemming from those accounts can be avoided.

☐ 83. Use stronger resources for better access control

Using classic resources can prove risky for your subscription.

AzureRM (v2) resources model provides stronger access control and auditing features.

☐ 84. Use stronger virtual machines on your subscription

Using new AzureRM (v2) enhances security with stronger access control, better auditing, access to managed identities, access to key vault for secrets, AAD-based authentication, support for tags and resource groups and much more.

☐ 85. Evaluate public IP addresses on the subscription

Public IPs allow direct internet access, exposing cloud resources to several types of attacks. So, there's a need for it to be verified thoroughly.

☐ 86. Limit hierarchy to three levels, including the root

Limit the management group depth to avoid confusion that hampers operations and security.

☐ 87. Increase the speed and scalability of your SIEM solution with a cloud-based SIEM

Investigate the features and capabilities of Azure security tools like Azure Sentinel and compare them with the capabilities of what you're currently using on-premises. Consider adopting Azure Sentinel if it meets your organization's requirements.

Azure Sentinel is a cloud-native Security Information and Event Management (SIEM) system, which empowers security professionals to face security challenges and threats that stem from your cloud as well as on premise sources.

☐ 88. Find most serious security vulnerabilities and prioritize investigation

Review your Azure secure score regularly to see recommendations resulting from the Azure policies and initiatives built into Azure Security Center.

☐ 89. Integrate Security Center alerts into your security information and event management (SIEM) solution

Processed events produced by Security Center are published to the Azure Activity Log, one of the logs available through Azure Monitor. Azure Monitor offers a consolidated pipeline for routing any of your monitoring data into a SIEM tool.

☐ 90. Integrate Azure logs with SIEM

Integrating Azure logs with SIEM is critical to enabling security incident investigation.

☐ 91. Enable Azure Policy

Enabling Azure Policy will ensure compliance with your company or regulatory security requirements by centrally managing security policies across your hybrid cloud workloads.

☐ 92. Identify roles responsible for monitoring policy violations

The assigned person must monitor compliance through the Azure portal or via the command line.

☐ 93. Map Azure policies to organizational policies for consistency

Map organization's documentation to the Azure policy by adding references.

☐ 94. Don't share credentials and other secrets on source code or GitHub

Don't let unauthorized parties gain access to your credentials. Attackers can take advantage of bot technologies to find keys and secrets stored in code repositories like GitHub.

☐ 95. Protect your keys

Azure Key Vault helps safeguard cryptographic keys and secrets that cloud applications and services use. With Key Vault, you can encrypt keys and secrets by using keys that are protected by hardware security modules.

☐ 96. Install anti-malware solution

Installing an anti-malware solution is a good practice to protect against malware.

☐ 97. Integrate antimalware with Azure Security Center

Integrating antimalware solution with Security Center helps you monitor the status of your own protection.

☐ 98. Store certificates in your key vault

Certificates are highly valuable and if it reaches the wrong hands, your application security or the security of your data can be at stake.

☐ 99. Ensure you can recover deleted key vaults or key vault objects

Deletion of key vaults or key vault objects can be inadvertent or malicious. Enable the soft delete and purge protection features of Key Vault, particularly for keys that are used to encrypt data at rest.

☐ 100. Use secure management workstation to protect sensitive accounts, tasks and data

Use a privileged access workstation to reduce the attack surface in workstations. These secure management workstations can help to mitigate attacks.

## How Azure cloud security professionals help protect your Azure environment

While securing Azure can run into several complications, if done well, it can keep your organization secure from the most malicious attacks. The Azure Security best practices checklist can be your guide in getting started, but to get the most of Azure Security, you'd require a team with training and technical knowledge.

Nuvento's cloud security professionals can guide you with the expertise you need to secure your data and systems. To know more, contact Nuvento's Azure experts today.